サイバーセキュリティ実践研修業務に係る情報提供依頼書（ＲＦＩ）

１　背景と目的

本県では、「広島県情報システム人材育成・確保プラン」に基づき、情報システム人材（デジタル専門人材）の育成に取り組んでいます。

この取組の一環として、当該人材に求められるサイバーセキュリティに関する知識及び技能の習得を図るとともに、情報セキュリティ対策の中核を担う人材を育成するため、実践的な研修の実施を検討しています。

ついては、研修内容、実施体制、概算費用等を把握するため、広く情報提供を依頼するものです。

２　情報提供依頼の実施方法

(1) 実施期間

令和８年９月９日（水曜日）から令和８年９月 25 日（金曜日）まで

(2) 提出を依頼する書類等

・様式１「サイバーセキュリティ実践研修業務情報提供依頼　回答書」

・必要に応じて、研修サービスの紹介資料、提案書、見積書その他の参考資料を併せて提出してください。既存の資料でも差し支えありません。

(3) 提出方法

「５　問い合わせ先」のメールアドレス宛に提出してください。

※メールサイズが 10MB を超える場合は、「５　問い合わせ先」にご相談ください。

・提出期限

令和８年９月 25 日（金曜日）17 時まで

(4) 質問方法

本情報提供依頼の内容について質問がある場合は、質問内容を記載した書面（任意様式）を「５　問い合わせ先」のメールアドレス宛に送信してください。

・質問期限

令和８年９月 16 日（水曜日）17 時まで

・回答方法

質問及び回答は、質問者を特定できる情報を除き、令和８年９月 18 日（金曜日）までに広島県公式ホームページに掲載します。

３　情報提供を依頼する内容

別紙「研修実施要件（案）」に対応可能な研修サービスについて、様式１により情報を提供してください。

なお、要件の一部について対応が困難な場合であっても、代替案の提案を妨げません。

４　留意事項

・　本情報提供依頼は、研修内容、実施体制、概算費用等を把握するために実施するものであり、契

約の相手方を選定するものではありません。

- 情報を提供いただいたことをもって、将来の契約を約束するものではありません。
- 情報提供に要する費用は、情報提供者の負担とします。
- 提供いただいた情報及び資料は、本県における事業内容及び調達方法の検討に使用します。情報提供者の承諾なく他の事業者等に提供することはありません。ただし、法令等に基づき開示を求められた場合を除きます。
- 提供いただいた情報及び資料は返却しません。
- 提供内容について、後日、確認又は追加の資料提供を依頼する場合があります。

５　問い合わせ先

広島県　総務局　デジタル基盤整備課　県・市町連携グループ（担当：塚本、藤井）
メール：soudgkiban@pref.hiroshima.lg.jp
電　話：０８２－５１３－２４３９（直通）

別紙

研修実施要件（案）

１　件名

令和８年度サイバーセキュリティ実践研修

２　研修の目的

本研修は、「広島県情報システム人材育成・確保プラン[1]」に基づき、広島県の情報職に求められるサイバーセキュリティに関する知識及び技能の習得を図るとともに、情報セキュリティ対策の中核を担う人材を育成することを目的とする。

このため、サイバー攻撃の手法及び脅威への理解を深め、将来的にペネトレーションテスト、脆弱性診断及びインシデントレスポンス等の高度なセキュリティ業務を担う専門人材の育成につながる実践的な基礎研修を実施する。

３　研修内容

本研修の受託者は、研修の企画、教材及び演習環境の準備、研修の実施、受講者支援、理解度確認並びに実施結果の報告を行うこと。

研修内容は、地方公共団体における情報システムの運用、セキュリティ対策及びインシデント対応を想定した事例を可能な限り取り入れたものとする。

また、研修の目的、期待される効果、実施体制、講師及び演習支援者、カリキュラム、タイムスケジュール、使用教材等を記載した実施計画書を作成し、あらかじめ広島県の承認を得ること。

４　研修の実施条件

(1)　受講対象者

情報職のうち、情報セキュリティ関連業務に従事する者とする。

(2)　定員

５名を予定する。ただし増減する場合がある。

(3)　実施日時・時間

研修は２日間とし、令和８年 10 月又は 11 月の実施を予定している。具体的な日程は、広島県と受託者が協議の上、決定する。

実施時間は、休憩時間を除き、２日間で計 12 時間程度とする。

(4)　開催形式

対面形式による集合研修とする。

(5)　実施場所

研修会場は広島県が用意し、広島県庁本庁舎内での実施を予定している。

ただし、研修効果又は演習環境上の理由から、受託者が用意する会場での実施が適当と考える場合は、会場、所在地、使用条件及び費用を提案することができる。

５　本業務で実施する研修及び演習

(1)　カリキュラム要件

研修は、将来的な高度セキュリティ人材の育成につながる実践的な内容とし、次に掲げる事項を体系的に含むこと。

---

[1] https://www.pref.hiroshima.lg.jp/soshiki/266/jyousysjinzai-ikuseiplan.html

ア　サイバーセキュリティの基礎及び倫理
・サイバー攻撃の代表的な手法及び攻撃プロセスに関する理解
・セキュリティ業務に従事する者としての倫理及び関連法令（不正アクセス行為の禁止等に関する法律その他関係法令）の理解
・Linux 及び Windows 環境における基本的なコマンドライン操作

イ　情報収集及び脆弱性分析
・公開情報を活用した情報収集及び分析の基本手法
・ネットワーク調査による稼働サービス及び OS の識別手法
・脆弱性情報データベース等を活用した脆弱性の調査及び分析手法

ウ　Web アプリケーションセキュリティ
・SQL インジェクション、クロスサイトスクリプティング等の代表的な脆弱性の仕組み及び対策
・脆弱性を悪用する攻撃の原理及び影響並びにその対策を理解するための実践的な演習
・認証・認可の不備及び設定不備に起因するリスクと対策

エ　脆弱性評価及び対策立案
・パスワード運用上の課題及び多要素認証の有効性に関する演習
・OS 及びミドルウェアの設定不備に起因する脆弱性に関する演習
・演習により発見した脆弱性について、影響度及び対応優先度を評価し、必要な対策を検討する演習

(2)　演習実施要件

本業務で実施する演習は、次の要件を全て満たすこと。

ア　基礎的な知識の習得に加え、実機操作を伴う演習を通じて、脆弱性の特定、評価及び対策の検討に必要となる基礎的な技能を習得できる内容であること。

イ　受託者は、研修の実施に必要な演習用端末、演習用仮想環境その他必要な機器及び環境を準備すること。受講者は、受託者が準備した環境を利用して演習を行うものとする。

なお、演習用仮想環境は、広島県及び第三者の情報システムに影響を及ぼさないよう、適切に分離された環境とすること。

ウ　近年の国内外における脅威動向及び攻撃手法に関する知見並びに実際の事例を反映し、実践的な知識及び技能を習得できる演習内容とすること。

エ　ポートスキャン、通信解析並びに脆弱性の特定及び検証等について、演習用仮想環境上で実践的な演習を実施すること。

６　研修における指導・運営体制要件

(1) 自治体セキュリティに関する知見

地方公共団体その他の公共機関における情報システム及びサイバーセキュリティ対策に関する知見又は支援実績を有し、自治体を取り巻くセキュリティ上の課題を踏まえた研修を実施できること。

(2) 演習運営体制

グループワーク等を活用し、受講者間の知識共有及び相互学習が図られるよう運営すること。

(3) 講師及び演習支援者

講師及び演習支援者は、サイバーセキュリティに関する十分な知識を有し、脆弱性診断、ペネトレーションテスト又はインシデント対応等の実務に従事した経験を有すること。

なお、情報処理安全確保支援士、CISSP、CEH、OSCP その他これらと同等以上の資格の保有者を

含むことが望ましい。

(4) 受講者支援

演習中の質問及び技術的な相談に速やかに対応できる支援体制を確保し、演習の進行に支援を要する受講者に対して、必要な助言及びフォローを行うこと。

7　研修後の評価及び成果物

(1) 理解度確認

研修で習得した知識及び技能の定着状況を確認するため、演習課題その他の方法による理解度確認を実施し、その結果を受講者への助言及び研修効果の検証に活用すること。

(2) 受講結果報告

受講者ごとの出席状況及び理解度確認結果を取りまとめ、広島県へ報告すること。

(3) 研修資料

講義資料、演習教材その他研修で使用した資料は、業務完了報告書の提出までに、電子データで提出すること。

(4) 修了証

所定のカリキュラムを修了した受講者に対し、受講内容及び研修修了を証する書類を交付すること。

8　費用

提示する費用には、講師及び演習支援者の旅費、教材費、演習用端末、演習環境利用料その他研修の実施に必要な一切の経費を含めること。